

REMARKS

1. Applicant thanks the Examiner for the Examiner's comments, which have greatly assisted Applicant in responding.

5

35 U.S.C. §103

3. Claims 1-40 are rejected by the Examiner under 35 U.S.C. §103(a) as being unpatentable over Vaid et al U.S. Patent No. 6,502,131 (hereinafter Vaid) in view of
10 Rogers et al U.S. Patent No. 5,557,747 (hereinafter Rogers).

Applicant respectfully disagrees. Applicant is of the opinion that a prima facie case of obviousness was not established because the three basic criteria were not met. Specifically and at least, the prior art of reference do not teach all the claim
15 limitations. Support follows hereinbelow.

(a) Claim 1 (and 13)

First, Applicant has amended Claim 1 (13) including incorporating limitations from
20 Claim 2 (14) and relying on page 9, lines 12-16 of the Specification to further clarify the invention. Amended Claim 1 appears as follows:

1. (currently amended) A system for analyzing network traffic to use in performing network and security assessments by listening on a subject network,
25 interpreting events, and taking action, comprising:
a policy specification file;
a network monitor processor for ~~processing~~ that processes network packet data collected from said subject network; and
a policy monitoring component ~~for receiving and processing~~ that receives
30 and processes said policy specification file[[,]] and that receives and processes ~~receiving and processing~~ said processed network packet data ~~to assign by~~ assigning dispositions to network events contained in said network packet data, wherein said policy monitoring component further comprises:
a parser that parses said policy specification file; and
35 a policy engine that synthesizes said parsed policy specification file and said processed network packet data and by comparing said processed network packet data against said parsed policy specification file, assigns associated dispositions and level of severity to said network events contained in

said network packet data wherein each of a plurality of network events that can occur in said subject network has an associated disposition.

Applicant specifically points out that neither prior art of reference teach at least the
5 limitation a policy engine that synthesizes said parsed policy specification file and
said processed network packet data and by comparing said processed network
packet data against said parsed policy specification file, assigns associated
dispositions and level of severity to said network events contained in said network
10 packet data wherein each of a plurality of network events that can occur in said
subject network has an associated disposition. As shown in the first response, Vaid
does not teach the limitation of assigning a disposition and level of severity.
Additionally, Vaid's policies are traffic policies, i.e. kinds of business, priority of
clients, properties of different applications being used, and so forth [15, Section 5].
15 Rogers disclose a policy can be described as a collection or set of statements that
direct a computer network program in response to changing network states as
signaled by events monitored within the network (Abstract.)

The Examiner has not shown where the prior art, alone or in combination, teach the
20 limitation of assigning dispositions and level of severity. Indeed, the Examiner has
not shown motivation for such nor reasonable expectation of success.

Accordingly, in view of the above, neither prior art of reference alone or in
combination teach, disclose, suggest, or motivate all claim limitations of Claims 1
and 13. Therefore, Claims 1 and 13 and the respective dependent claims, are in
25 condition for allowance. Applicant respectfully requests that the Examiner withdraw
the rejection under 35 U.S.C. §103(a).

(b) Claim 33 (and 25)

30 Applicant has amended Claim 33 (25) to incorporate the policy monitor component of
Claim 1 (13). Therefore, in view of the amendment and in view of the above, neither
prior art of reference alone or in combination teach, disclose, suggest, or motivate all
claim limitations of Claims 33 and 25. Therefore, Claims 33 and 25 and the
respective dependent claims, are in condition for allowance. Applicant respectfully
35 requests that the Examiner withdraw the rejection under 35 U.S.C. §103(a).

4. It should be appreciated that Applicant has elected to amend the Claims
solely for the purpose of expediting the patent application process in a manner

- consistent with the PTO's Patent Business Goals, 65 Fed. Reg. 54603 (9/8/00). In making such amendment, Applicant has not and does not in any way narrow the scope of protection to which Applicant considers the invention herein to be entitled. Rather, Applicant reserves Applicant's right to pursue such protection at a later point in time and merely seeks to pursue protection for the subject matter presented in this submission.
- 5

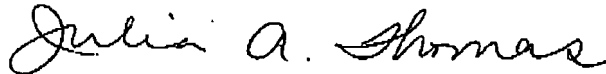
CONCLUSION

5 Based on the foregoing, Applicant considers the present invention to be distinguished from the art of record. Accordingly, Applicant earnestly solicits the Examiner's withdrawal of the rejections raised in the above referenced Office Action, such that a Notice of Allowance is forwarded to Applicant, and the present application is therefore allowed to issue as a United States patent. The Examiner is invited to call to discuss the response.

10

Respectfully Submitted,

15



Julia A. Thomas
Reg. No. 52,283

20

Customer No. 22862